

Micro-segmentation strategies reveal divergences across Europe

Adoption is now widespread, but motivations, priorities
and approaches differ from one market to another

Study conducted by Censuswide among 400 IT and cybersecurity decision-makers
in France, Germany, the United Kingdom and the Netherlands

Introduction

At a time when expectations around resilience, compliance and sovereignty are pushing European companies to rethink their architecture, while facing significant constraints in terms of cost, integration and user experience, they agree on one principle for protecting their data: **sensitive information must be isolated from the rest and hosted in separate environments.**

Micro-segmentation, which consists of partitioning an information system into isolated environments, has thus established itself in recent years as **a cornerstone of cybersecurity strategies.**

While a majority of European companies have already deployed it or are in the process of doing so (86%), **their motivations, approaches and the difficulties they encounter vary considerably from one country to another.**

Some are primarily driven by regulatory requirements; others place greater emphasis on operational, resilience or technological sovereignty considerations.

More broadly, opinions also diverge on medium-term priorities, particularly on the place given in IT security strategies to micro-segmentation and its last link, the workstation.

Beyond European trends, this study highlights the most significant gaps observed between markets and offers **a particular focus on the position of France.**

The results notably reveal **a more proactive approach to security**, a distinctive relationship with regulation, and priorities that, on several topics, clearly set it apart from its European neighbours.

> Methodology

The study was conducted by Censuswide among a sample of 400 senior managers and executives (middle management and above), aged 21 and over, in the United Kingdom, France, the Netherlands and Germany (100 respondents per country). Respondents work in IT, cybersecurity, infrastructure, compliance or data protection roles within companies with 250 or more employees, and have held their current position for at least one year.

Sectors represented include engineering, IT, finance, construction, defence, energy, healthcare, manufacturing, transport & travel, and the public sector. Data was collected from 7 to 12 August 2026.

Censuswide is a member of the Market Research Society (MRS) and the British Polling Council (BPC), and a signatory of the Global Data Quality Pledge. The institute abides by the MRS Code of Conduct and ESOMAR principles.

400

decision-makers surveyed

4 countries

100 respondents each

Summer 2026

data collection

> 02 – ADOPTION

A consensus on principle, an uneven implementation

86%

have already deployed micro-segmentation
or are in the process

83%

consider the workstation as
a specific focus area

4.5%

have no plans to deploy it

To contain the risk of lateral spread in the event of an attack, most companies apply micro-segmentation: 86% of the companies surveyed have already deployed it (45%) or are in the process of doing so (41%). Only 4.5% say it is not on their agenda. But the study shows that **this adoption is not yet accompanied by a shared implementation standard.**

In practice, virtualisation (53%), VPN (52.5%) and dedicated physical workstations (50%) are the most commonly used methods, either alone or in combination. In other words, the rise of virtualisation and VPNs has not led to the abandonment of the historical approach: **the dedicated workstation remains a key lever in segmentation strategies.**

The importance given to the workstation is also reflected in the way organisations now design their segmentation. For 83% of respondents, **the workstation is a fully-fledged focus area of their IT segmentation strategy.**

This level of recognition is consistent from one country to another, with rates ranging from 76% to 89% depending on the market. **The question is no longer whether the workstation should be part of the segmentation strategy, but how.**

Each country has its own strategy: the Netherlands stands out as the most mature and homogeneous market (few laggards, strong adoption of virtualisation), while Germany remains the most attached to historical methods (dedicated workstations) and France appears to favour VPN as its main partitioning lever, more so than virtualisation.

The United Kingdom is a case apart: it is both the most advanced country in terms of virtualisation and the one with the most companies lacking any separation strategy, **a sign of a polarised market rather than a uniformly mature one.**

THREE METHODS, NO DOMINANT STANDARD



MICRO-SEGMENTATION



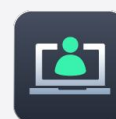
VIRTUALISATION
ISOLATED ENVIRONMENTS

53%



VPN
ACCESS ISOLATION

52.5%



DEDICATED WORKSTATION
PHYSICAL SEPARATION

50%

> 03 – BARRIERS & COMPLIANCE

Organisational rather than technological barriers

One of the clearest lessons from the study is that **adoption difficulties are not due to a lack of solutions on the market**. The main obstacles to adoption cited by respondents are administrative complexity (50% overall, 62% in Germany) and implementation cost (50%), far ahead of the lack of suitable solutions, mentioned by only 25% of them.

In other words, decision-makers do not consider the market offering to be insufficient. Their main concern is rather **the ability to deploy, administer and maintain these systems over time** without excessively increasing costs or the operational burden on teams.

This finding suggests that **the challenge is now more organisational than technological**. **Solutions exist**, but their adoption remains conditional on their ease of deployment, their integration into existing environments and their operational cost.

For vendors, the challenge is therefore no longer just to demonstrate the effectiveness of their technology, but also **their ability to reduce the complexity associated with implementing it**.

Regulatory compliance: the main driver, with nuances

50%

cite implementation complexity

50%

cite cost as the main obstacle

25%

cite the lack of suitable solutions

Behind the near-total consensus around micro-segmentation, **motivations differ significantly from one market to another**.

Germany appears to be the country most strongly driven by regulatory requirements, with particular weight given to the GDPR (58%) and national regulations (43.5%). **The Netherlands, for its part, stands out for the influence of NIS2 (44%) and DORA (35%)**, reflecting the importance attached to European regulatory frameworks.

This regulatory sensitivity may be due to different factors depending on the country. In Germany, for example, the institutional structure is the mirror image of France's.

Unlike France, which has a single national authority, **Germany relies on a network of federal and regional authorities** (Länder), contributing to a more visible presence of compliance issues within companies.

> 04 - THE FRENCH SPECIFICITY

French companies are more driven by internal choices

48%

cite workstation security

46%

cite technological sovereignty

45%

cite NIS2 and DORA compliance

When it comes to micro-segmentation, French companies stand out neither for a particularly high level of maturity nor for a notable delay. What sets them apart lies rather in the factors driving their projects: **initiatives there are primarily guided by internal strategic choices rather than by regulatory constraints.**

Indeed, **it is the only one of the four countries studied** where internal strategic decision-making (51%) ranks ahead of the GDPR (43%) among the main drivers of segmentation. While compliance is the dominant trigger for their neighbours, French organisations seem to be driven more by an internal vision and strategic choices.

This suggests that in France, information system segmentation is perceived **less as an obligation to be met than as a lever for risk control.** In other words, whereas regulation often acts as a catalyst elsewhere in Europe, French companies appear more inclined to frame these initiatives as part of **a security approach driven by their own operational priorities.**

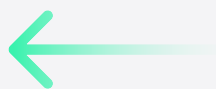
This approach is also reflected in the hierarchy of security priorities. While the United Kingdom continues to make micro-segmentation its number one security priority, **France now seems to be shifting its attention to other issues** such as workstation security (48%), technological sovereignty (46%) and NIS2 and DORA compliance (45%).

The methods used today to partition sensitive environments also confirm this French specificity, with 60% of organisations relying on VPN, compared with 43% in the United Kingdom. This strong adoption of VPN may reflect a pragmatic approach by French companies: **strengthening access isolation without abandoning existing systems.**

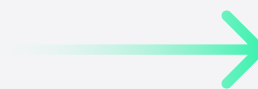
THE FRENCH MODEL



INTERNAL CHOICE
51%



MICRO-SEGMENTATION



VPN
60%

> 05 – THE NEXT TWELVE MONTHS

Priorities for the next 12 months: the French exception

36%

of French decision-makers cite micro-segmentation

69%

of British decision-makers list micro-segmentation among their priorities

33

point gap between France and the United Kingdom

Across Europe, **the same security priorities** emerge for the next twelve months: IT micro-segmentation (47%), technological sovereignty (46.5%), workstation security (46%), NIS2/DORA compliance (45%) and identity management (41%) all fall within a very narrow range.

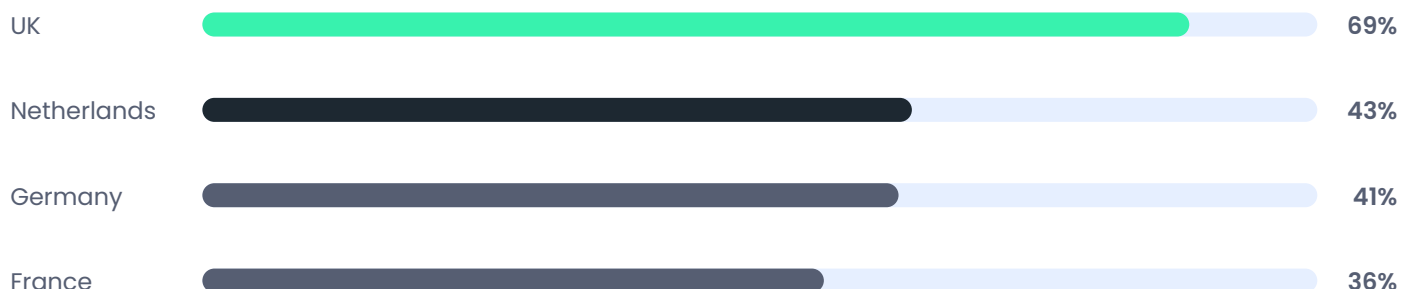
Behind this apparent convergence, however, lies **the most pronounced gap in the entire study**. In France, only 36% of decision-makers cite micro-segmentation among their priorities for the next 12 months, compared with 69% in the United Kingdom, a difference of 33 points. The gap is much smaller with the Netherlands (43%) and Germany (41%), which points less to a French singularity than to **a specific divergence between France and the United Kingdom**.

This difference does not, however, seem to reflect a delay in adoption. With 83% of deployments completed or under way, France shows a level of adoption comparable to that observed in the other countries studied (85% to 89%).

The most plausible interpretation is that of **a market that considers it has already come most of the way** and is now **turning its attention to other issues**.

In France, the challenge is no longer just to segment, but to make better use of and monitor the environments already deployed

> 12-month micro-segmentation priority



Dependence on non-European solutions: often a deliberate choice... and contradictions

81%

use non-European solutions

55%

use non-European solutions by choice

51%

would not be influenced by European origin

81% of the companies surveyed rely on non-European solutions to address their security and compliance challenges. This dependence is particularly marked in Germany (88%) and the Netherlands (86%).

While digital sovereignty is among companies' stated priorities, **it still carries little weight in concrete decisions**. More than one in two organisations (55%) using non-European solutions **do so by choice**, and only 23% due to a lack of identified alternatives.

The contrast is even sharper when it comes to purchasing: 51% of decision-makers believe that **the European origin of a suitable alternative would have no influence on their decision**, while only 26.5% would consider it a decisive factor.

This gap suggests that while digital sovereignty is widely acknowledged in strategic discourse, it ultimately carries little weight in purchasing decisions. Faced with operational criteria such as ease of deployment, cost or integration with existing systems, **sovereignty often takes a back seat**.

On this subject, **German manufacturers stand out**. They are the most inclined to reconsider their position: 40% say they would be strongly influenced, the highest level in this sector. Conversely, their British counterparts remain largely indifferent to this argument, with 67% saying it would not factor into their decision "at all". Where the British seem to accept the situation, German manufacturers would see the emergence of European alternatives as **an opportunity to reduce their dependence**.

Finally, **French manufacturers take a more "measured" position**. While their dependence on non-European suppliers is just as high as that of their neighbours, **it is more often endured than chosen**: only 20% of respondents say they chose it. Yet French manufacturers are **reluctant to switch suppliers in favour of a European alternative**. Less than a third (27%) say they are sensitive to the European origin of an alternative.

FROM DISCOURSE TO DECISION



STATED
SOVEREIGNTY



OPERATIONAL TRADE-OFFS



COST



PERFORMANCE



INTEGRATION

> 07 - OT ENVIRONMENT

OT focus: how industry stands out from the rest of the French economy

In France, the industrial sector (construction, energy and manufacturing) stands out clearly from the rest of the French economy in the importance it gives to the workstation. **More than eight out of ten decision-makers (82%) make it a 12-month priority, almost double the figure for other sectors (44%).**

In the same vein, **100% of French industrial respondents (11 out of 11)** make the workstation a specific focus area of their segmentation strategy, compared with 85% for the rest of the country.

Finally, internal decision-making is particularly strong there: **78% of industrial respondents say they act primarily on the impetus of their own strategy, compared with 43% for other sectors.**

This result confirms that, in industry, segmentation is seen more as **an operational and resilience issue** than as a mere response to regulatory requirements.

The French industrial sector: a special case

While industry everywhere tends to pay particular attention to securing the workstation, **France takes this logic much further than its neighbours. The gap between industrial and other sectors reaches 38 points**, compared with 26 points in the Netherlands and 21 points in the United Kingdom. Germany is the only market where no difference appears (50% in both cases).

Here, France shows by far **the largest gap of the four markets studied.**

> Conclusion

This study shows a European market in full transition towards a more mature approach to information system segmentation. **The relevance of micro-segmentation is no longer in question**, but its adoption drivers remain shaped by national contexts. While regulatory requirements continue to play a structuring role in several countries, **France approaches it more from the angle of internal strategy.**

At the same time, sovereignty is emerging as a subject of reflection, **without becoming a decisive criterion in most purchasing decisions.** Trade-offs remain strongly guided by operational considerations such as cost, performance or integration with existing architecture.

Beyond national divergences, one finding stands out: organisations are now looking for approaches capable of **reconciling compliance, operational simplicity and control over technological dependencies.** In this context, **the workstation emerges as a point of convergence** within a broader reflection on information system micro-segmentation and, by extension, on the protection of sensitive data.